Encryption

Exercise 5.1 (🤝/📝/🏠)

1. Split into working groups of 3 or 4 students
2. Each group is assigned one of the topics (by consensus or randomization) described on the following slides
3. Every group prepares a digital presentation of 15-20min on their topic
4. At least *2 days before* the presentation a PDF export of the slides is uploaded on Moodle (once per group)
5. All groups present their topic to all their classmates who can ask questions afterwards

Presentation Format

- 15-20 minutes presentation
  - *every* group member *has to* present for at least 5min
- ~5 minutes Q&A

ℹ️ *The presentation can be written and held in* 🇬🇧 *or* 🇩🇪 *based on each group's own preference. Just do not mix English and German slides. English slides but presentation held in German is fine.*

Presentation Topics

1. WEP ⚡ FMS & Chopchop
2. WPA2 ⚡ KRACK
3. PGP ⚡ EFAIL
4. SSL/TLS ⚡ POODLE & DROWN
5. BitLocker ⚡ TCG Opal
6. PDF ⚡ Breaking Encryption & Signatures

💡 *The links provided are some documentation/specification (if publicly available) as well as vulnerability research papers. Each group is supposed to gather additional references as needed.*

Presentation Structure

1. Introduction of the protocol/system
2. Explanation of the attack(s)
3. Mitigation of the attack(s)
4. Recommendations or related information

ℹ️ *Please provide a list of sources referred to in the presentation as the final slide.*

Timeline

- Tue, 15.11.2021 *(today)*
  - Group building & topic assignment
- Sun, 04.12.2021 *(+3 weeks)*
  - All PDF-exported presentations uploaded on Moodle
- **Tue, 06.12.2021** *(+2 days)*
  - **All groups present their topics** between 15:00 and 17:30